PHNL 021017

Europäisches Patentamt
European Patent Office
Office européen des brevets

20/529664

IB/03/4344

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

02079154.7

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 02079154.7
Demande no:

Anmeldetag:
Date of filing: 03.10.02
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Method for reversible embedding

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G06F1/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR

Method for reversible embedding

FIELD OF THE INVENTION

This invention disclosure addresses the problem of embedding information for high quality restoration in a lower quality signal, where the signal is typically an audio-visual signal.

BACKGROUND OF THE INVENTION

One of the proposed methods for Digital Rights Management (DRM) of high quality audio content involves making only low quality versions available to unlicensed users. Licensed users however are provided with some additional information, typically a cryptographic key, that allows them access to an additional quality layer, so as to obtain the original high quality content. Typically the additional quality layer is provided as a separate and encrypted bitstream, i.e. separate from the low quality bit stream. An example of such a dual layer quality approach can be found in the DRM methods being proposed for DVD-Audio.

The presence of two separate bit streams poses a security risk because the encrypted high quality layer is easily traceable, and therefore accessible for cryptographic attacks. For example, by playing out the high quality layer of DVD-Audio, an attacker can try to exploit the observed relation between the encrypted and decrypted bit streams for retrieving cryptographic keys.

OBJECT AND SUMMARY OF THE INVENTION

To overcome the sketched problem we propose to multiplex the low quality and high quality layer into a single bitstream This is done in such a way that the multiplexed bitstream has only minimal distortion with respect to the low quality layer. The high quality layer is embedded in this minimal distortion of the low quality layer and can be made available by providing a proper decoder. The theoretical bounds that can be achieved with respect to distortion and rates are provided in appendix 1.

An (admittedly) toy example of how this can be achieved involves a simple scalar quantizer Q_1 and a more sophisticated vector quantizer Q_2 that have the same rate. In this setup a source X can be quantized with the high quality quantizer Q_2. That means that every coding vector x in X is approximated by a vector $q_2(k)$, for some index k. As Q_1 and Q_2 have the same number of coding vectors, it is possible to find a reordering r(k) such that $q_1(r(k))$ is also an approximation to x, although in general of less quality. An unlicensed user will then be given a set of indices with respect to the scalar quantizer Q_1 and he will be able to reconstruct a low quality approximation to X. A licensed user will have access to the code vectors in Q_2 as well as the inverse of the reordering map r(k) and will therefore be able to reconstruct a better approximation to X. An example of such an double quantizer construct is provided in appendix 2.

DESCRIPTION OF EMBODIMENTS

These and other aspects of the invention are apparent from and will be elucidated, by way of a non-limitative example, with reference to the embodiment(s) described in the appendices

Throughout the figures, same reference numerals indicate similar or corresponding features. Some of the features indicated in the drawings are typically implemented in software, and as such represent software entities, such as software modules or objects.

Although the invention has been described with reference to particular illustrative embodiments, variants and modifications are possible within the scope of the inventive concept. Thus, for example,

The use of the verb 'to comprise' and its conjugations does not exclude the presence of elements or steps other than those defined in a claim. In the claims, any reference signs placed between parentheses shall not be construed as limiting the claim. The invention can be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer. In the device claim enumerating several means, several of these means can be embodied by one and the same item of hardware.

A 'computer program' is to be understood to mean any software product stored on a computer-readable medium, such as a floppy-disk, downloadable via a network, such as the Internet, or marketable in any other manner.

While the invention has been described in connection with preferred embodiments, it will be understood that modifications thereof within the principles outlined above will be evident to those skilled in the art, and thus the invention is not limited to the preferred embodiments but is intended to encompass such modifications. The invention resides in each and every novel characteristic feature and each and every combination of characteristic features. Reference numerals in the claims do not limit their protective scope. Use of the verb "to comprise" and its conjugations does not exclude the presence of elements other than those stated in the claims. Use of the article "a" or "an" preceding an element does not exclude the presence of a plurality of such elements. 'Means' , as will be apparent to a person skilled in the art, are meant to include any hard-ware (such as separate or integrated circuits or electronic elements) or soft-ware (such as programs or parts of programs) which perform in operation or are designed to perform a specified function, be it solely or in conjunction with other functions, be it in isolation or in co-operation with other elements.

Reversible Embedding Methods

Frans Willems and Ton Kalker
Philips Research Laboratories and Eindhoven University, Eindhoven
f.m.j.willems@tue.nl, ton.kalker@ieee.org

Abstract

We consider embedding of messages (data-hiding) into i.i.d. source (host) sequences. As in [7] and [8] we focus on the case where reconstruction of the source sequence is desired. Instead of complete reconstruction however we investigate the case where there is only partial reconstruction (restoration) needed. Embedding has an effect on the rate of the composite sequence. This effect is taken into account in our investigations. The optimal trade-off between embedding rate, composite rate, distortion between source sequence and composite sequence, and distortion between source sequence and restoration sequence is given by the admissible region. This admissible region is determined here.

1 Introduction

A side effect of many watermarking and data-hiding methods is that the source (host) signal into which messages are embedded is distorted. Finding the optimal trade-off between the amount of information embedded and the induced distortion is therefore an active field of research. In recent years, with the rediscovery (see e.g. [10] and [3]) of Costa's seminal paper "Writing on Dirty Paper" [5], there has been considerable progress in understanding the fundamental limits of the capacity versus distortion of watermarking and data-hiding schemes. For some applications no distortion resulting from embedding messages is allowed. In these cases the use of reversible data-hiding methods provide a way out. A reversible data-hiding method is defined as a scheme that allows blind recovery of the original host data. A reversible scheme was proposed by Fridrich et al. [7]. Recently theoretical progress has been made in understanding the limits of reversible watermarking in terms of rate versus distortion [8]. It is the purpose of the present paper to investigate embedding in the case where only partial reconstruction is required.

2 System description

Consider a source that produces a sequence $x_1^N = (x_1, x_2, \cdots, x_N)$ of N independent and identically distributed (i.i.d.) symbols, i.e. for some distribution $\{Q(x), x \in \mathcal{X}\}$

$$\Pr\{X_1^N = x_1^N\} = \Pi_{n=1,N} \Pr\{X_n = x_n\} = \Pi_{n=1,N} Q(x_n), \qquad (1)$$

for all $x_1^N \in \mathcal{X}^N$ where $\mathcal{X}$ is the (finite) source alphabet. The positive integer N is called the block-length. Into the source sequence x_1^N a message index w is embedded. This message

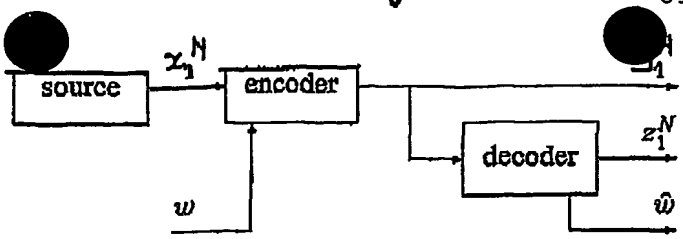


Figure 1: A general embedding system.

index assumes values in $\{1, 2, \cdots, M\}$ and is independent of the source sequence x_1^N and uniformly distributed, hence

$$\Pr\{W = w\} = 1/M, \text{ for all } w \in \{1, 2, \cdots, M\}. \tag{2}$$

The encoder (embedder) maps each source sequence x_1^N together with the message index w to a sequence $y_1^N = (y_1, y_2, \cdots, y_N)$, referred to as a *composite* sequence. This composite sequence y_1^N consists of N components from the finite composite alphabet $\mathcal{Y}$. We write

$$y_1^N = e(x_1^N, w) = \left(e_1(x_1^N, w), e_2(x_1^N, w), \cdots, e_N(x_1^N, w)\right), \tag{3}$$

where $e(\cdot, \cdot)$ is the encoder mapping and $e_n(\cdot, \cdot)$ for $n = 1, N$ are its projections.

Observing the composite sequence y_1^N the decoder determines a *restoration* sequence $z_1^N = (z_1, z_2, \cdots, z_N)$ of symbols from the finite alphabet $\mathcal{Z}$, thus

$$z_1^N = f(y_1^N) = \left(f_1(y_1^N), f_2(y_1^N), \cdots, f_N(y_1^N)\right), \tag{4}$$

where $f(\cdot)$ is the decoder mapping and where for $n = 1, N$, $f_n(\cdot)$ is the corresponding n^{th} projection.

Moreover the decoder produces an estimate $\hat{w}$ of the message index that was embedded, thus

$$\hat{w} = g(y_1^N). \tag{5}$$

This estimate assumes values in $\{1, 2, \cdots, M\}$.

The expected distortion between the composite sequence y_1^N and the source sequence x_1^N is defined as

$$\overline{D_{xy}} \triangleq \frac{1}{N} \sum_{x_1^N} \sum_{w} \sum_{n=1,N} \Pr\{X_1^N = x_1^N\} \Pr\{W = w\} D_{xy}\left(x_n, e_n(x_1^N, w)\right), \tag{6}$$

for some matrix $D_{xy}(\cdot, \cdot)$, and where generally $\overline{D_{xy}}$ is expected to be small. We assume that the matrix $D_{xy}(\cdot, \cdot)$ contains non-negative finite entries only.

The composite sequence y_1^N is compressed on the basis of its first order entropy. This leads to two possible definitions for a composite rate, where $R_c = H(Y)$ is an obvious choice. Another option, in particular in applications where y_1^N is obtained from a scalar quantizer, is to use symbol-by-symbol coding, using the same binary prefix code for all N symbols. If the codeword lengths in binary symbols are $\{l(y), y \in \mathcal{Y}\}$, then he corresponding composite rate R_a is then defined as

$$R_a = L_H(Y) \triangleq \frac{1}{N} \sum_{x_1^N} \sum_{w} \sum_{n=1,N} \Pr\{X_1^N = x_1^N\} \Pr\{W = w\} l\left(e_n(x_1^N, w)\right). \tag{7}$$

definition; however all results presented will still hold true with $L_H(Y)$ replaced by $H(Y)$ in case of non-symbol-by-symbol encoding. In generally the rate R_c should be as small as possible.

Also the expected distortion between source sequence x_1^N and restoration sequence z_1^N has to be small, and is defined as

$$\overline{D_{xz}} \triangleq \frac{1}{N} \sum_{x_1^N} \sum_{n=1,N} \sum_{w} \Pr\{X_1^N = x_1^N\} \Pr\{W = w\} D_{xz}\left(x_n, f_n\left(e(x_1^N, w)\right)\right) \tag{8}$$

for some matrix $D_{xz}(\cdot, \cdot)$ that contains non-negative finite entries only.

Of course, the number of allowed messages M, expressed by the embedding rate R_e

$$R_e \triangleq \frac{1}{N} \log_2 M, \tag{9}$$

should be as large as possible.

Finally the average error probability P_e, defined as

$$P_e \triangleq \sum_{x_1^N = g(a(x_1^N, w))} \Pr\{X_1^N = x_1^N\} \Pr\{W = w\}, \tag{10}$$

should be as small as possible.

3 Main result

Now that we have described a general embedding system we can proceed to the main result of this paper, the admissible region for general embedding. First we have to define admissibility. Following standard practice, we define a quadruple $(\rho_e, \rho_c, \Delta_{xy}, \Delta_{xz})$ to be admissible if for all $\epsilon > 0$ there is a number N_ϵ such that for all $N > N_\epsilon$ there exist encoders and decoders such that

$$\begin{aligned} R_e &\geq \rho_e - \epsilon, \\ R_c &\leq \rho_c + \epsilon, \\ \overline{D_{xy}} &\leq \Delta_{xy} + \epsilon, \\ \overline{D_{xz}} &\leq \Delta_{xz} + \epsilon, \\ P_e &\leq \epsilon. \end{aligned} \tag{11}$$

In the following sections we will prove the following result:

Theorem 1 *A set $\mathcal{R} = \{(\rho_e, \rho_c, \Delta_{xy}, \Delta_{xz})$ of quadruples is admissable if and only if there exists a joint probability distribution $P(x, y, z) = Q(x)P(y, z|x)$ such that*

$$\begin{aligned} &\rho_c \geq H(Y), \\ &0 \leq \rho_e \leq H(Y) - I(X; Y, Z), \\ &\Delta_{xy} \geq \mathrm{E}_{xy}[D_{xy}(x, y)], \\ &\Delta_{xz} \geq \mathrm{E}_{xz}[D_{xz}(x, z)], \end{aligned}$$

where $H(Y)$ is the binary entropy of the marginal distribution $P(y)$ and where $\mathrm{E}[\cdot]$ is the expectation operator.

The following two sections will proof this result. The easy part, i.e. the converse, is done first in Section 4. The more involved part, i.e. achievability, is done in Section 5.

Given an general embedding system as in Figure 1 we first define the joint distribution (X, Y, Z). To this end, consider the random variable I assuming values from $\{1, 2, \cdots, N\}$ with probability $1/N$, independently. Next define the conditional single letter random variables

$$(X, Y, Z|I = n) \triangleq (X_n, Y_n, Z_n). \tag{12}$$

Note that now the probability distribution for (X, Y, Z) is given by:

$$\Pr\{(X, Y, Z) = (x, y, z)\} = \frac{1}{N} \sum_{n=1,N} \Pr\{(X_n, Y_n, Z_n) = (x, y, z)\}, \tag{13}$$

for $x \in \mathcal{X}$, $y \in \mathcal{Y}$, and $z \in \mathcal{Z}$. Note that for this joint probability $P(x, y, x)$ we can write $P(x, y, z) = Q(x)P(y, z|x))$.

The proof now proceeds in a number of steps. We start by by using Fano's inequality to get a lower bound on the rate R_e in terms of the conditional probability $H(W|Y_1^N, Z_1^N, \hat{W})$.

$$\begin{aligned} H(W|Y_1^N, Z_1^N, \hat{W}) &\leq H(W|\hat{W}) \\ &\leq h(P_e) + P_e \log_2(M-1) \leq 1 + P_e N R_e, \end{aligned} \tag{14}$$

where $h(\alpha) = -\alpha \log_2 \alpha - (1-\alpha)\log_2(1-\alpha)$ for $0 \leq \alpha \leq 1$ is the binary entropy function. From this we obtain

$$\begin{aligned} \sum_{n=1,N} H(Y_n) \geq H(Y_1^N) &= H(Y_1^N, Z_1^N, \hat{W}) \\ &= H(Y_1^N, Z_1^N, \hat{W}, W) - H(W|Y_1^N, Z_1^N, \hat{W}) \\ &\geq H(Y_1^N, Z_1^N, \hat{W}, W) - 1 - P_e N R_e \\ &= H(Y_1^N, Z_1^N, W) - 1 - P_e N R_e, \end{aligned} \tag{15}$$

Another step

$$\begin{aligned} H(Y_1^N, Z_1^N, W) &= H(W) + H(Y_1^N, Z_1^N|W) \\ &\geq H(W) + I(Y_1^N, Z_1^N; X_1^N|W) \\ &= N R_e + H(X_1^N|W) - H(X_1^N|Y_1^N, Z_1^N, W) \\ &\geq N R_e + H(X_1^N) - H(X_1^N|Y_1^N, Z_1^N) \\ &= N R_e + \sum_{n=1,N} H(X_n) - \sum_{n=1,N} H(X_n|Y_1^N, Z_1^N, X_1^{n-1}) \\ &\geq N R_e + \sum_{n=1,N} H(X_n) - \sum_{n=1,N} H(X_n|Y_n, Z_n). \end{aligned} \tag{16}$$

Combining (15) and (16) we obtain

$$\sum_{n=1,N} H(Y_n) \geq (1 - P_e) N R_e - 1 + \sum_{n=1,N} H(X_n) - \sum_{n=1,N} H(X_n|Y_n, Z_n). \tag{17}$$

Note that by (12) inequality (17) can be rewritten as

$$H(Y|I) \geq (1 - P_e) R_e - 1/N + H(X|I) - H(X|Y, Z, I), \tag{18}$$

$$H(Y) \geq (1 - P_e)R_e - 1/N + H(X) - H(X|Y, Z). \tag{19}$$

Note that an admissible $\rho_e \leq R_e + \epsilon$ for $\epsilon \downarrow 0$ and $N \to \infty$. Therefore for admissible ρ_e we obtain

$$\rho_e \leq H(Y) - I(X; Y, Z), \tag{20}$$

for some joint distribution $P(x, y, z) = Q(x)P(y, z|x), x \in \mathcal{X}, y \in \mathcal{Y}, z \in \mathcal{Z}$.

Next we consider the composite rate:

$$\begin{aligned} NR_c &= \sum_{y_1^N} \Pr\{Y_1^N = y_1^N\} \sum_{n=1,N} l(y_n) \\ &= \sum_{n=1,N} \sum_{y} \Pr\{Y_n = y\} l(y) \\ &= N \sum_{y} \Pr\{Y = y\} l(y) \\ &\geq N L_H(Y). \end{aligned} \tag{21}$$

Here the last step follows from the fact that the Huffman code is optimal, i.e. minimizes the expected codeword length. Recall that an admissible ρ_c satisfies $\rho_c \geq R_c - \epsilon$ for $\epsilon \downarrow 0$, hence $\rho_c \geq L_H(Y)$.

Finally for the distortions we obtain:

$$\begin{aligned} \overline{D_{xy}} &= \sum_{x_1^N, y_1^N} \Pr\{(X_1^N, Y_1^N) = (x_1^N, y_1^N)\} \frac{1}{N} \sum_{n=1,N} D_{xy}(x_n, y_n) \\ &= \frac{1}{N} \sum_{n=1,N} \sum_{x,y} \Pr\{(X_n, Y_n) = (x, y)\} D_{xy}(x, y) \\ &= \sum_{x,y} \Pr\{(X, Y) = (x, y)\} D_{xy}(x, y), \end{aligned} \tag{22}$$

and

$$\begin{aligned} \overline{D_{xz}} &= \sum_{x_1^N, z_1^N} \Pr\{(X_1^N, Z_1^N) = (x_1^N, z_1^N)\} \frac{1}{N} \sum_{n=1,N} D_{xz}(x_n, z_n) \\ &= \frac{1}{N} \sum_{n=1,N} \sum_{x,z} \Pr\{(X_n, Z_n) = (x, z)\} D_{xz}(x, z) \\ &= \sum_{x,z} \Pr\{(X, Z) = (x, z)\} D_{xz}(x, z), \end{aligned} \tag{23}$$

Finally note that admissible distortions satisfy $\Delta_{xy} \geq D_{xy} - \epsilon$ and $\Delta_{xz} \geq D_{xz} - \epsilon$ for $\epsilon \downarrow 0$, which proves the result.

5 Outline of the achievability proof

This proof is based on strong typicality, see e.g. Cover and Thomas [6], p. xxx. Fix $\{P(y, z|x), x \in \mathcal{X}, y \in \mathcal{Y}, z \in \mathcal{Z}\}$. This determines the joint distribution $P(x, y, z) = Q(x)P(y, z|x)$. Next fix a $\delta > 0$ and a block-length N.

We define
typical x-sequences x_1^N defined by

$$1-\delta \leq \frac{\#(x|x_1^N)}{NQ(x)} \leq 1+\delta, \tag{24}$$

for all $x \in \mathcal{X}$, where $\#(x|x_1^N)$ denotes the number of occurrences of x in x_1^N. Then

$$\Pr\{X_1^N \notin \mathcal{A}_\delta^N(X)\} \leq \delta \tag{25}$$

for all N large enough.

B. Note that $P(y|x) = \sum_z P(y,z|x)$ for $x \in \mathcal{X}, y \in \mathcal{Y}$. Now consider for each $x_1^N \in \mathcal{A}_\delta^N(X)$ the set $\mathcal{A}_\delta^N(Y|x_1^N)$ of y-sequences y_1^N typical with x_1^N, i.e. sequences for which the actual number of (x,y) pairs is close to the expected number. More formally, we require

$$1-\delta \leq \frac{\#(x,y|x_1^N,y_1^N)}{\#(x|x_1^N)P(y|x)} \leq 1+\delta, \tag{26}$$

for all $x \in \mathcal{X}, y \in \mathcal{Y}$. Now it can be shown that, for all $x_1^N \in \mathcal{A}_\delta^N(X)$, for all N large enough, the size of the set $\mathcal{A}_\delta^N(Y|x_1^N)$ is lower bounded by

$$|\mathcal{A}_\delta^N(Y|x_1^N)| \geq 2^{N[(1-\delta)^2 H(Y|X)-\delta]}. \tag{27}$$

Moreover, for all $y_1^N \in \mathcal{A}_\delta^N(Y|x_1^N)$ the average distance $d(x_1^N,y_1^N)$ is close to the expected distance as expressed by

$$d(x_1^N,y_1^N) \triangleq \frac{1}{N}\sum_{n=1,N} D_{xy}(x_n,y_n) \leq (1+\delta)^2\,\mathrm{E}_{xy}[D_{xy}(x,y)]. \tag{28}$$

C. Next let $P(z|x,y) = P(y,z|x)/\sum_z P(y,z|x)$ for $x \in \mathcal{X}, y \in \mathcal{Y}, z \in \mathcal{Z}$. Now consider for each $x_1^N \in \mathcal{A}_\delta^N(X)$ and $y_1^N \in \mathcal{A}_\delta^N(Y|x_1^N)$ the set $\mathcal{A}_\delta^N(Z|x_1^N,y_1^N)$ of z-sequences z_1^N typical with (x_1^N,y_1^N), i.e. sequences for which the actual number of (x,y,z) pairs is close to the expected number. More formally, we require

$$1-\delta \leq \frac{\#(x,y,z|x_1^N,y_1^N,z_1^N)}{\#(x,y|x_1^N,y_1^N)P(z|x,y)} \leq 1+\delta, \tag{29}$$

for all $x \in \mathcal{X}, y \in \mathcal{Y}, z \in \mathcal{Z}$. Now it can be shown that, for all $x_1^N \in \mathcal{A}_\delta^N(X)$ and $y_1^N \in \mathcal{A}_\delta^N(Y|x_1^N)$, for all N large enough, the size of the set $\mathcal{A}_\delta^N(Z|x_1^N,y_1^N)$ is lower bounded by

$$|\mathcal{A}_\delta^N(Z|x_1^N,y_1^N)| \geq 2^{N[(1-\delta)^3 H(Z|X,Y)-\delta]}. \tag{30}$$

Moreover for all $z_1^N \in \mathcal{A}_\delta^N(Z|x_1^N,y_1^N)$ the average distance $d(x_1^N,z_1^N)$ is close to the expected distance as expressed by

$$d(x_1^N,z_1^N) \triangleq \frac{1}{N}\sum_{n=1,N} D_{xz}(x_n,z_n) \leq (1+\delta)^2\,\mathrm{E}_{xz}[D_{xz}(x,z)]. \tag{31}$$

D. Next consider the sequences $y_1^N \in \mathcal{A}_\delta^N(Y|x_1^N)$ for some $x_1^N \in \mathcal{A}_\delta^N(X)$. Give each such sequence y_1^N a random message-label w, i.e.

$$\Pr\{W(y_1^N) = w\} = \frac{1}{M} \text{ for } w \in \{1,\cdots,M\}, \tag{32}$$

according to distribution $P(z|y) = \sum_x P(x,y,z)/\sum_{x,z} P(x,y,z)$. Denote this sequence by $z_1^N(y_1^N)$. Now for $y_1^N \in \mathcal{A}_\delta^N(Y|x_1^N)$ where $x_1^N \in \mathcal{A}_\delta^N(X)$ we get that

$$\Pr\{Z_1^N \in \mathcal{A}_\delta^N(Z|x_1^N, y_1^N)\} \geq 2^{-N[(1+\delta)^3 H(Z|Y)-(1-\delta)^3 H(Z|X,Y)+\delta]}. \tag{33}$$

E. The encoder, when it receives a source sequence $x_1^N \notin \mathcal{A}_\delta^N(X)$, declares an error. When the encoder receives a source sequence $x_1^N \in \mathcal{A}_\delta^N(X)$ and message w as inputs, it produces a composite sequence y_1^N that satisfies

$$\begin{aligned} y_1^N &\in \mathcal{A}_\delta^N(Y|x_1^N) \\ w(y_1^N) &= w, \\ z_1^N(y_1^N) &\in \mathcal{A}_\delta^N(Z|x_1^N, y_1^N). \end{aligned} \tag{34}$$

When no y_1^N satisfying (34) exists an error is declared. Also when an error error is declared the encoder still produces a composite sequence (albeit arbitrary) and the decoder still forms a restoration sequence.

G. There are two kinds of errors: (i) the source can generate an $x_1^N \notin \mathcal{A}_\delta^N(X)$, or (ii) for $x_1^N \in \mathcal{A}_\delta^N(X)$ there may not be an y_1^N satisfying (34).

H. The first probability P_e^i can be made smaller than δ by increasing N, see (25). If $x_1^N \in \mathcal{A}_\delta^N(X)$ the probability that a specific $y_1^N \in \mathcal{A}_\delta^N(Y|x_1^N)$ has the right message label and that $Z_1^N(y_1^N) \in \mathcal{A}_\delta^N(Z|x_1^N, y_1^N)$, is not smaller than $2^{-N[(1+\delta)^3 H(Z|Y)-(1-\delta)^3 H(Z|X,Y)+\delta]}/M$, see bound (33) hence

$$\begin{aligned} P_e^{ii} &\leq \prod_{y_1^N \in \mathcal{A}_\delta^N(Y|x_1^N)} \left(1 - \frac{2^{-N[(1+\delta)^3 H(Z|Y)-(1-\delta)^3 H(Z|X,Y)+\delta]}}{M}\right) \\ &= 2^{\sum_{y_1^N \in \mathcal{A}_\delta^N(Y|x_1^N)} \log_2\left(1-\frac{2^{-N[(1+\delta)^3 H(Z|Y)-(1-\delta)^3 H(Z|X,Y)+\delta]}}{M}\right)} \\ &\leq 2^{\sum_{y_1^N \in \mathcal{A}_\delta^N(Y|x_1^N)} -\frac{2^{-N[(1+\delta)^3 H(Z|Y)-(1-\delta)^3 H(Z|X,Y)+\delta]}}{M \ln 2}} \\ &\leq 2^{-N\delta}, \end{aligned} \tag{35}$$

if for all $x_1^N \in \mathcal{A}_\delta^N(X)$

$$\frac{|\mathcal{A}_\delta^N(Y|x_1^N)| 2^{-N[(1+\delta)^3 H(Z|Y)-(1-\delta)^3 H(Z|X,Y)+\delta]}}{M} \geq 2^{N\delta}. \tag{36}$$

Note that this holds if we take

$$M = 2^{N[(1-\delta)^2 H(Y|X)-(1+\delta)^3 H(Z|Y)+(1-\delta)^3 H(Z|X,Y)-2\delta]}. \tag{37}$$

Now we let $\delta \downarrow 0$ and $N \to \infty$. This yields the admissibility of

$$\begin{aligned} \rho_s &= H(Y|X) - H(Z|Y) + H(Z|X,Y) \\ &= H(X,Y) - H(X) - I(X;Z|Y) \\ &= H(X,Y) - H(X) - H(X|Y) + H(X|Y,Z) \\ &= H(Y) - I(X;Y,Z). \end{aligned} \tag{38}$$

I. The admissible distortions are what they should be. This is easily checked, since the distortion matrices D_{xy} and D_{xz} contain only non-negative finite entries, since $P_e^i + P_e^{ii}$ tends to zero for $\delta \downarrow 0$ and $N \to \infty$, and since the bounds (28) and (31) hold when x_1^N, y_1^N, and z_1^N are jointly typical. Note that the composite rate $L_H(Y)$ is admissible since y_1^N is typical with probability tending to one for $\delta \downarrow 0$ and $N \to \infty$.

Theorem 1 is a quite general result on embedding of information. To understand the consequences of this theorem better, we consider some special cases.

The important feature in all cases is that the embedding of information results in a distortion and that this distortion should be small. Therefore in all setups there is an embedding rate and a distortion between the source an composite sequences. The differentation follows from putting different requirements on the distortion of the restoration sequence. We consider three cases here: (i) standard embedding, (ii) reversible embedding, and (iii) self-embedding. Standard embedding refers to the case where we put no restriction on the restoration sequence and is discussed in Section 6.1. Reversible embedding requires that the restoration sequence has zero distortion with the source sequence and is discussed in Section 6.2. The last scenario refers to a scenario where do not put any constraint on the embedding rate. The relevance of such a scenario is discussed in Section 6.3.

6.1 Standard embedding

In this case we assume that random variable Z is not present and that there is no distortion matrix $D_{xz}(\cdot,\cdot)$. This immediately yields the following achievable region

$$\begin{aligned}\mathcal{R} = \{(\rho_e, \rho_c, \Delta_{xy}) \;:\; & 0 \leq \rho_e \leq H(Y|X), \\ & \rho_c \geq H(Y), \\ & \Delta_{xy} \geq \mathrm{E}_{xy}[D_{xy}(x,y)],\end{aligned} \tag{39}$$

where entropies and expectations are with respect to some joint probability function $P(x,y) = Q(x)P(y|x), x \in \mathcal{X}, y \in \mathcal{Y}$. If we are not interested in the value of the composite rate ρ_c we obtain

$$\begin{aligned}\mathcal{R} = \{(\rho_e, \Delta_{xy}) \;:\; & 0 \leq \rho_e \leq H(Y|X), \\ & \Delta_{xy} \geq \mathrm{E}_{xy}[D_{xy}(x,y)],\end{aligned} \tag{40}$$

Note that this last situation was considered by Chen [2] and Barron [1]. They called this the noise-free case to emphasize that the composite signal is not modified e.g. during transmission over a noisy channel. In [13] codes for noise-free embedding in gray-scale signals were considered.

6.2 Reversible embedding

We assume here that we complete restoration is required, i.e. we want to reconstruct the source sequence x_1^N reliably. Therefore we just take $Z = X$. This leads to

$$\begin{aligned}\mathcal{R} = \{(\rho_e, \rho_c, \Delta_{xy}) \;:\; & 0 \leq \rho_e \leq H(Y) - H(X), \\ & \rho_c \geq L_H(Y), \\ & \Delta_{xy} \geq \mathrm{E}_{xy}[D_{xy}(x,y)],\end{aligned} \tag{41}$$

where entropies and expectations are with respect to some joint probability function $P(x,y) = Q(x)P(y|x), x \in \mathcal{X}, y \in \mathcal{Y}$. If we are not interested in the value of the composite rate ρ_c we obtain

$$\begin{aligned}\mathcal{R} = \{(\rho_c, \Delta_{xy}) \;:\; & 0 \leq \rho_e \leq H(Y) - H(X), \\ & \Delta_{xy} \geq \mathrm{E}_{xy}[D_{xy}(x,y)],\end{aligned} \tag{42}$$

Goljan and Du in [7]. They proposed a more or less ad-hoc method for reversible embedding of data in images. This method is suboptimal in two ways, (a) it does not consider the host symbol as side-information during embedding, nor (b) does it reconstruct the host sequence conditionally on the composite signal. Coding techniques that improve upon the method of Fridrich et al. [7] will be presented in [9].

6.3 Self-embedding

In this setup it is not our intention to embed message-information but only to restore a better estimation of the source sequence x_1^N from a 'bad' estimation y_1^N.

A simple example of such a setup would be the case where x_1^N is compressed to obtain a sequence z_1^N within a distortion Δ_{xz}. By (partially) encrypting or hashing z_1^N a composite sequence y_1^N is obtained with a (in general)larger distortion Δ_{xy}. By controlling the degree of encryption both the rate and the distortion of the composite sequence can be controlled. In this view we depart from a simple rate-distortion setup. As an index to the restoration sequence z_1^N, the encoder can transmit a sequence of symbols that are meaningful, and not just some string of abstract symbols. Such a meaningful index is the sequence y_1^N, which is close to the source sequence x_1^N, close in terms of a distortion measure. The advantage of this setup is now that when errors occur during transmission of y_1^N the symbols that were correctly received are still informative. Restoration is not possible however.

In a more information-theoretic view we have quantized version y_1^N of the source sequence x_1^N and this sequence contains information to do a restoration. This restoration leads to z_1^N. An additional property of this approach could be that only a legitimate user could do the restoration, for example when the restoration decoder is controlled by a secret key.

The optimal trade-off between composite rate and the expected distortion is expressed by the admissible region

$$\begin{aligned} \mathcal{R} = \{(\rho_c, \Delta_{xy}, \Delta_{xz}) \;:\; & \rho_c \geq H(Y), \\ & \Delta_{xy} \geq \mathrm{E}_{xy}[D_{xy}(x,y)], \\ & \Delta_{xz} \geq \mathrm{E}_{xz}[D_{xz}(x,z)] \end{aligned} \tag{43}$$

where entropies and expectations are with respect to some joint probability function $P(x,y,z) = Q(x)P(y,z|x), x \in \mathcal{X}, y \in \mathcal{Y}, z \in \mathcal{Z}$ such that $H(Y) \geq I(X;Y,Z)$.

7 Final remarks

The setup that we have studied here is somewhat related to the problem that was investigated by Sutivong et al. [11], [12]. However their problem concerns transmission, ours is an embedding problem. We want the distortion between source and composite sequence to be small whereas Sutivong et al. have a side-information channel that determines what will be received.

The concept of "stealing bits from a quantized source" see [4] is related to our setup via its objective. Also Cohen et al. want to embed information by allowing (extra) distortion.

References

[1] R.J. Barron, *Systematic Hybrid Analog/Digital Signal Coding*, Ph.D. dissertation, Massachusetts Inst. of Techn., June 2000.

Data Hiding Systems, Ph.D. dissertation, Massachusetts Inst. of Techn., June 2000.

[3] B. Chen and G.W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inform. Theory,* vol. IT-47, pp. 1423-1443, May 2001.

[4] A.S. Cohen,

[5] M.H.M. Costa, "Writing on dirty paper," *IEEE Trans. Inform. Theory,* vol. IT-29, pp. 439-441, May 1983.

[6] T.M. Cover and J.A. Thomas, *Elements of Information Theory.* Wiley, New York, 1991.

[7] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding for all image formats," *Proc. SPIE, Security and Watermarking of imedia Contents,* San Jose, California, 2002.

[8] T.Kalker and F.M.J. Willems, "Capacity bounds and constructions for reversible data-hiding," *Proc. Int. Conf. DSP,* Santorini, Greece, July 1-3, 2002.

[9] D. Maas, T. Kalker, and F. Willems, "A code construction for recursive reversible data-hiding," to be presented at *iets van de ACM,* December 5, 2002, Juan-les-Pins, France.

[10] P. Moulin and J. O'Sullivan, "Information-theoretic Analysis of Information Hiding," preprint, 1999.

[11] A. Sutivong, T.M. Cover, and M. Chiang, "Trade-off between message and state information rates," *Proc. ISIT 2001,* Washington DC, June 24 - 29, 2001, p. 303.

[12] A. Sutivong, T.M. Cover, M. Chiang, and Young-Han Kim, "Rate vs. distortion trade-off for channels with state information," *Proc. ISIT 2002,* Lausanne, Switzerland, June 30 - July 5, 2002, p. 226.

[13] F.M.J. Willems and M. van Dijk, "Codes for embedding information in grayscale signals," *Proceedings 39th Allerton Conference,* October 1-3, 2001, Monticello, Illinois.

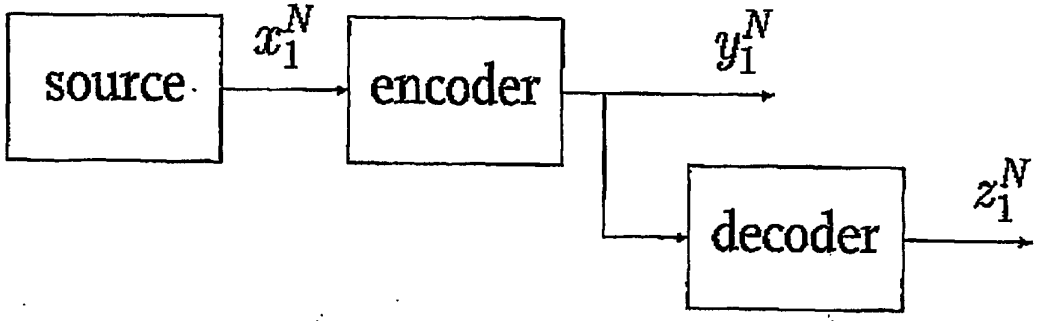
TU/e technische universiteit eindhoven

SELF-EMBEDDING
or
Embedding reconstruction information of a vector quantiser in a scalar quantiser

Ton Kalker and Frans Willems

Eindhoven University of Technology, Eindhoven, The Netherlands
Philips Research Laboratories, Eindhoven, The Netherlands

1. System description



The source is memoryless, i.e. for some distribution $\{Q(x), x \in \mathcal{X}\}$

$$\Pr\{X_1^N = x_1^N\} = \Pi_{n=1,N} Pr\{X_n = x_n\} = Q(x_n). \tag{I.1}$$

The encoder produces the sequence y_1^N from x_1^N, therefore

$$y_1^N = f(x_1^N) = f_1(x_1^N), f_2(x_1^N), \cdots, f_N(x_1^N). \tag{I.2}$$

The expected distortion between y_1^N and x_1^N is defined as

$$\overline{D_{xy}} \triangleq \sum_{x_1^N} \Pr\{X_1^N = x_1^N\} \frac{1}{N} \sum_{n=1,N} D_{xy}(x_n, f_n(x_1^N)), \tag{I.3}$$

for some matrix $D_{xy}(\cdot,\cdot)$, and should be small.

The sequence y_1^N is compressed symbol-by-symbol, using the same prefix code for all N symbols. The codeword lengths are $\{l(y), y \in \mathcal{Y}\}$. The quantiser rate

$$R_q = \sum_{x_1^N} \Pr\{X_1^N = x_1^N\} \frac{1}{N} \sum_{n=1,N} l(f_n(x_1^N)), \tag{I.4}$$

should be as small as possible.
From the sequence y_1^N the decoder (reconstructor) determines another sequence z_1^N thus

$$z_1^N = g(y_1^N) = g_1(y_1^N), g_2(y_1^N), \cdots, g_N(y_1^N). \tag{I.5}$$

Also the expected distortion between x_1^N and z_1^N has to be small, it is defined as

$$\overline{D_{xz}} \triangleq \sum_{x_1^N} \Pr\{X_1^N = x_1^N\} \frac{1}{N} \sum_{n=1,N} D_{xz}(x_n, g_n(f(x_1^N))) \tag{I.6}$$

for some matrix $D_{xz}(\cdot, \cdot)$,

TU/e technische universiteit eindhoven

2. Admissible region

The triple $(\rho, \Delta_{xy}, \Delta_{xz})$ is admissible if for all $\epsilon > 0$ there exists for all N large enough encoders and decoders such that

$$\begin{aligned} R &\leq \rho + \epsilon \\ \overline{D_{xy}} &\leq \Delta_{xy} + \epsilon \\ \overline{D_{xz}} &\leq \Delta_{xz} + \epsilon. \end{aligned} \qquad (2.1)$$

It can be shown that the set $\mathcal{R}$ of admissible triples satisfies

$$\begin{aligned} \mathcal{R} = \{(\rho, \Delta_{xy}, \Delta_{xz}) \ : \ & \rho \geq H(Y), \\ & \Delta_{xy} \geq \sum_{x,y,z} Q(x) P(y,z|x) D_{xy}(x,y), \\ & \Delta_{xz} \geq \sum_{x,y,z} Q(x) P(y,z|x) D_{xz}(x,z), \\ & \text{for some } \{P(y,z|x), x \in \mathcal{X}, y \in \mathcal{Y}, z \in \mathcal{Z}\} \\ & \text{such that } H(Y) \geq I(X;Y,Z)\}. \end{aligned} \qquad (2.2)$$

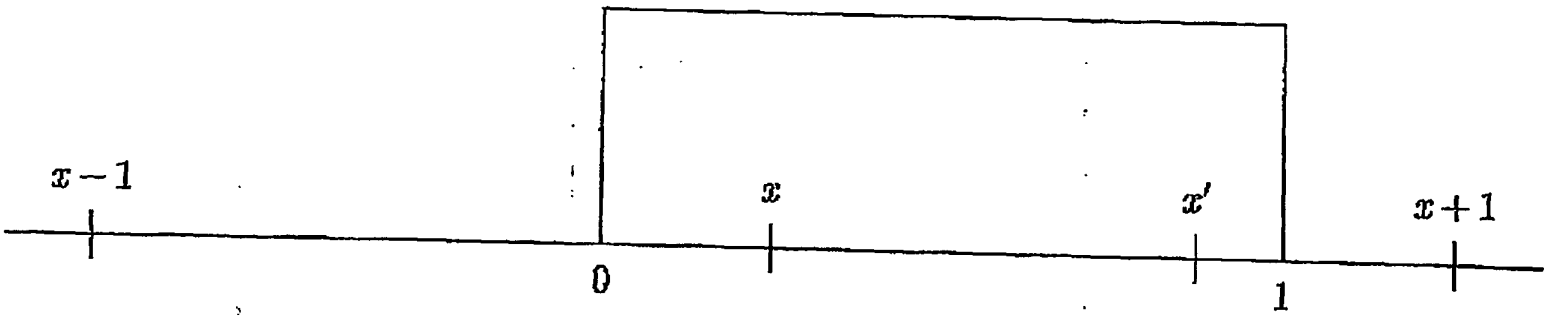
3. An example

A source signal, circular-mean-square-error distortion

Consider a signal x. Its range is $[0, 1)$, its density is uniform.
When the signal x is replaced by another signal $x' \in [0, 1)$ the distortion is

$$D(x, x') = \min[(x' - x + 1)^2, (x' - x)^2, (x' - x - 1)^2]. \tag{3.1}$$

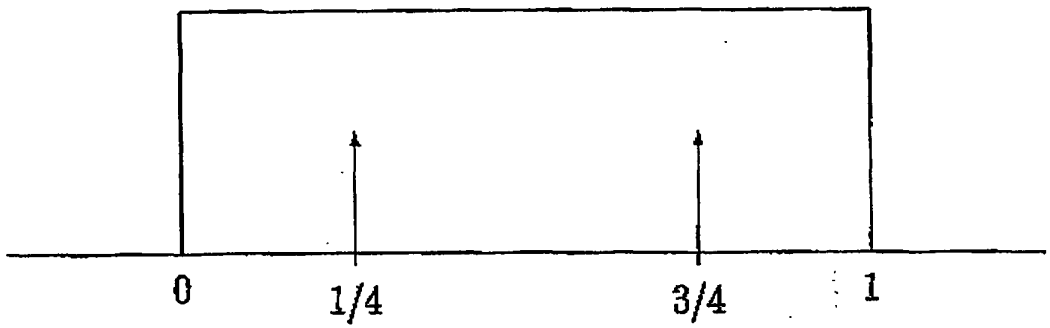
We call this measure circular-mean-square-error distortion. Think of this signal as lying on a circle, with circumference 1, etc.



This setup gives us the opportunity to ignore boundary effects when studying uniform quantization.

A scalar quantizer

We now quantize each sample x to either $1/4$ or $3/4$. The quantized signal y is $1/4$ for $x < 1/2$ and $3/4$ for $x \geq 1/2$. See figure.



The mean-square-error distortion that is induced by this quantizer is

$$D_s = \frac{1}{48} = 0.0208. \tag{3.2}$$

The rate of this scalar quantizer is

$$R_s = 1 \text{ bit per sample.} \tag{3.3}$$

A vector quantizer

We can also quantize N samples x_1^N together into z_1^N. Take $N = 4$ and consider the following "code" with 16 sequences $z_1^N(i)$ for $i = 0, 15$:

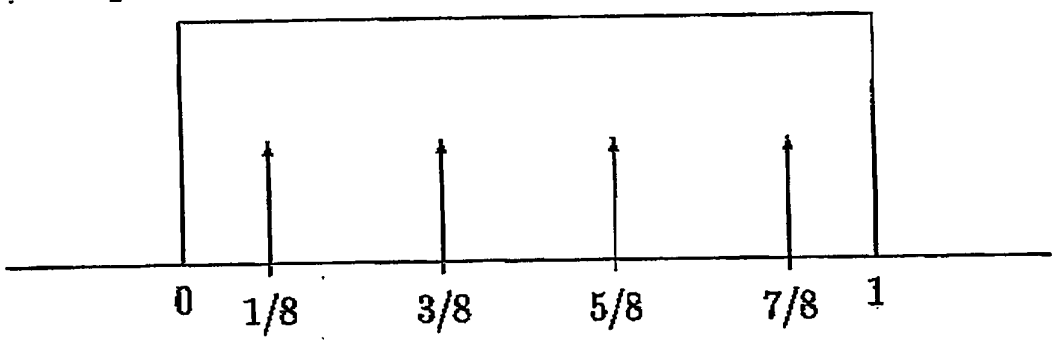
i	z_1	z_2	z_3	z_4	i	z_1	z_2	z_3	z_4
0	1/8	1/8	1/8	1/8	8	7/8	1/8	3/8	5/8
1	1/8	3/8	5/8	7/8	9	7/8	3/8	7/8	3/8
2	1/8	7/8	5/8	3/8	10	7/8	7/8	7/8	7/8
3	1/8	5/8	1/8	5/8	11	7/8	5/8	3/8	1/8
4	3/8	1/8	7/8	5/8	12	5/8	1/8	5/8	1/8
5	3/8	3/8	3/8	3/8	13	5/8	3/8	1/8	7/8
6	3/8	7/8	3/8	7/8	14	5/8	7/8	1/8	3/8
7	3/8	5/8	7/8	1/8	15	5/8	5/8	5/8	5/8

Simulations show that this code yields a distortion

$$D_v \approx 0.0197, \tag{3.4}$$

while the rate is again

$$R_v = \frac{\log_2 16}{4} = 1 \text{ bit per sample.} \tag{3.5}$$



The improvement over scalar quantization is not very large, only 0.25 dB. Note however that the code is short.

Using the scalar quantizer N times

Again assume that $N = 4$. Then there are 16 possible sequences y_1^N that can occur if the scalar quantizer is used for all four samples x_1, x_2, x_3, x_4. We list these sequences $y_1^N(j)$ for $j = 0, 15$:

j	y_1	y_2	y_3	y_4	j	y_1	y_2	y_3	y_4
0	1/4	1/4	1/4	1/4	8	3/4	1/4	1/4	1/4
1	1/4	1/4	1/4	3/4	9	3/4	1/4	1/4	3/4
2	1/4	1/4	3/4	1/4	10	3/4	1/4	3/4	1/4
3	1/4	1/4	3/4	3/4	11	3/4	1/4	3/4	3/4
4	1/4	3/4	1/4	1/4	12	3/4	3/4	1/4	1/4
5	1/4	3/4	1/4	3/4	13	3/4	3/4	1/4	3/4
6	1/4	3/4	3/4	1/4	14	3/4	3/4	3/4	1/4
7	1/4	3/4	3/4	3/4	15	3/4	3/4	3/4	3/4

A one-to-one mapping, encoding

Our method is now as follows:
A sequence x_1^N is quantized by the vector quantizer. This yields sequence $z_1^N(i)$ for some i. Consider now a one-to-one mapping $m(\cdot)$ such that $j = m(i)$. This mapping is used to replace $z_1^N(i)$ by the "scalar-quantized" sequence $y_1^N(m(i))$. Instead of $z_1^N(i)$ the sequence $y_1^N(m(i))$ is sent to the decoder, symbol-by-symbol.
Can we now choose this mapping $m(\cdot)$ in such a way that the distortion D_{xy} between x_1^N and y_1^N is small?
Computer simulations show that the mapping

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$j = m(i)$	0	1	6	5	3	2	4	7	9,	10	15	12	8	11	13	14

gives a distortion

$$D_{xy} \approx 0.0473, \tag{3.6}$$

Remember that the rate $R = 1$ bit per sample.

Decoding

The decoder can

- either use the scalar-quantized sequence y_1^N, that was sent to him directly, for reconstruction. In this way a distortion $D_{xy} \approx 0.0473$ is achieved,
- or use the inverse $m^{-1}(\cdot)$ to obtain the index $i = m^{-1}(j)$. This results in the sequence z_1^N and the much smaller distortion $D_{xz} \approx 0.0197$.

PHNL021017 CPP 25 03.10.200

TU/e technische universiteit eindhoven

How good is this?

4. Why should we do this?

1. The inverse mapping $m^{-1}(\cdot)$ can be kept secret for unauthorized users. Such an unauthorized user does obtain a quantized sequence with a poor performance however. An authorized user achieves a good performance.

2. If in transmission of y_1^N errors occur, parts of the sequence y_1^N can still be used for reconstruction.

3. Note that embedding vector information in a scalar quantizer does not cost a thing.

CLAIMS:

1. A method to reconstruct an improved approximation 'Z' of a host signal 'X' from a lower quality approximation 'Y', such that

a) 'Y' assumes values that could have been produced by a first quantizer 'Q1', and

b) 'Z' is obtained from 'Y' by interpreting the quantization indices of 'Q1' as indices for a second quantizer 'Q2', where 'Q2' is possibly dependent on 'Y', and possibly in conjunction with a reordering map of the indices.

2. A method as in claim 1, where 'Q1' is a scalar quantizer and 'Q2' is a vector quantizer.

3. A method as in claim 1, where high quality reconstruction ingredients are hidden from unlicensed users:

a) The quantizer 'Q2' is hidden from unlicensed users;

b) The reordering map is hidden from unlicensed users.

4. An apparatus comprising circuitry for implementing the steps of a method as claimed in any one of claims 1 to 3.

5. A computer program product enabling a programmable device when executing said computer program product to function as an apparatus as defined in claim 4.

ABSTRACT:

This invention disclosure addresses the problem of embedding information for high quality restoration in a lower quality signal, where the signal is typically an audio-visual signal.